PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to implement procedures to ensure verification that a workforce member or entity seeking access to Electronic Protected Health Information (ePHI) is the one claimed. When implementing technical safeguards MDHHS shall execute processes to corroborate that an entity or individual is who or what they claim to be. The authentication process may occur through any reasonable and appropriate trusted process such as, but not limited to, the use of secret passwords, personal identification number, digital certificate or a token.

REVISION HISTORY

Reviewed: 01/01/2022.
Next Review: 01/01/2023.

DEFINITIONS

Digital Certificate is a file that includes the name and email address of the certificate holder, dates of validity and an encryption key that can be used to verify the digital signature of the holder and the name of the issuing company. Most commonly used in SSL or secure socket layer on ecommerce sites.

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

PHI is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

Token means a small device that displays a constantly changing ID code. A user first enters a password and then the card displays an ID that can be used to login a network.

Workforce Member means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

POLICY

It is the policy of MDHHS that workforce members seeking access to any network, system or application that contains ePHI must satisfy a user authentication mechanism such as unique user identification and password, biometric input or a user identification smart card to verify their authenticity.

PROCEDURE

Workforce Member

A reasonable effort must be made to verify the identity of the receiving person or entity prior to transmitting ePHI.

Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's user ID and password, smart card, digital signatures or other authentication information when seeking access to any network, system or application.

Workforce members are not permitted to allow other persons or entities to use their unique user ID and password, smart card, or other authentication information.

Division Director or Section Supervisor/Manager

MDHHS shall include in its authentication processes documented procedures for:

- Granting persons and entities authentication credentials or for changing an existing authentication method.
- Detecting and responding to any person or entity attempting to access ePHI without proper authentication.

REFERENCES

45 CFR 164.312(d)

CONTACT

For additional information concerning this policy and procedure, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.